Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented): A method for authenticating a hardcopy document, comprising the steps of:

recording in a memory a scanned representation of the hardcopy document at a selected resolution;

generating lossy compressed image data with the scanned representation of the hardcopy document;

producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

arranging in the memory the scanned representation of the hardcopy document with a digital encoding of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

2. (original): The method according to claim 1, further comprising the step of verifying the signed hardcopy document by:

recording a scanned representation of the signed hardcopy document;

decoding the authentication token from the scanned representation of the signed hardcopy document;

authenticating the lossy compressed image data using one of the encrypted image data and the hashed encrypted image data; and

decompressing the authenticated lossy compressed image data for comparison with the signed hardcopy document to determine whether the signed hardcopy document is authentic.

3. (original): The method according to claim 2, further comprising the step of visually comparing the signed hardcopy document with the authenticated lossy compressed image data.

4. (original): The method according to claim 2, further comprising the step of visually comparing the signed hardcopy document with a printed hardcopy document of the authenticated lossy compressed image data.

5. (original): The method according to claim 2, wherein said step of producing an authentication token is performed with a private key and said step of authenticating lossy compressed image data is performed with a public key.

6. (original): The method according to claim 1, further comprising the step of encoding the authentication token in a low intensity background pattern.

7. (original): The method according to claim 1, further comprising the step of encoding the authentication token in embedded data.

8. (original): The method according to claim 7, wherein said encoding step encodes the authentication token in a halftone pattern.

9. (original): The method according to claim 8, wherein said encoding step encodes the authentication token in a hyperbolic halftone pattern.

10. (original): The method according to claim 8, wherein said encoding step encodes the authentication token in a serpentine halftone pattern.

11. (original): The method according to claim 7, wherein said encoding step encodes the authentication token in data glyphs.

12. (original): The method according to claim 1, wherein said step of generating lossy compressed image data loses document formatting contained in the scanned representation of the hardcopy document.

13. (original): The method according to claim 12, wherein said step of generating lossy compressed image data further comprises the step of compressing the scanned representation of the hardcopy document by identifying exemplars and locations of exemplars; each exemplar identified representing one or more image segments from the scanned representation of the hardcopy document.

14. (original): The method according to claim 13, wherein said compressing step records the exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document.

15. (currently amended): The method according to claim 13, wherein said compressing step records [[that]] the locations of exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document.

16. (currently amended): The method according to ~~claim 1~~ claim 13, wherein said compressing step compresses identified portions of the image [[data]] segments at a plurality of compression ratios.

17. (original): The method according to claim 16, further comprising the step of segmenting text data from pictorial data before compressing the scanned representation of the hardcopy document.

18. (currently amended): A method for authenticating a hardcopy document, comprising the steps of:

recording in a memory a scanned representation of the hardcopy document at a selected resolution;

generating lossy compressed image data with the scanned representation of the hardcopy document;

producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy

compressed image data and an encrypted hash of the lossy compressed image data; and

arranging in the memory a digital encoding of the authentication [[data]] token for rendering at a printer a label containing the digital encoding of the authentication [[data]] token.

19. (original): The method according to claim 18, further comprising the step of fixedly attaching the label to the hardcopy document to produce a signed hardcopy document.

20. (original): The method according to claim 19, further comprising the step of verifying the signed hardcopy document by:

recording a scanned representation of the signed hardcopy document;

decoding the authentication token from the scanned representation of the signed hardcopy document;

authenticating the lossy compressed image data using one of the encrypted image data and the hashed encrypted image data; and

decompressing the authenticated lossy compressed image data for comparison with the signed hardcopy document to determine whether the signed hardcopy document is authentic.

21. (previously presented): A system for authenticating a scanned representation of a hardcopy document, comprising:

an image compression module for generating lossy compressed image data with the scanned representation of the hardcopy document;

an authentication token generator for producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

an encoding module for arranging the scanned representation of the hardcopy document with a digital encoding of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

22. (currently amended): The system according to Claim 21, further comprising:

a memory for recording the signed hardcopy document;

a decoding module for decoding the signed hardcopy document to define decoded signed image data;

an authentication module [[to]] for authenticating the ~~decided~~ decoded signed image data using [[of]] the encrypted image data and the hashed encrypted image data to define authenticated image data; and

a decompression module for decompressing the authenticated image data to define decompressed image data;

means for comparing the signed hardcopy document with the authenticated hardcopy document to determine whether the signed hardcopy document is authentic.

23. (previously presented): The system according to Claim 21, wherein said image compression module compresses the scanned representation of the hardcopy document by identifying exemplars and locations of exemplars; each exemplar identified representing one or more image segments from the scanned representation of the hardcopy document.